Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen Tietoliikenne ja tietoturva

2014

Saku Nuutinen ja Hans Lindström

TIETOTURVAKARTOITUS PK-YRITYKSILLE

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yritysten tietoliikenne ja tietoturva

2014 | 42 sivua

Esko Vainikka

Saku Nuutinen ja Hans Lindström

TIETOTURVAKARTOITUS PK-YRITYKSILLE

Tämän opinnäytetyön tavoitteena on auttaa yritystä tunnistamaan tietoturvariskinsä, parantaa sitä kautta yleisesti toiminnan tehokkuutta ja luoda järkeviä hallintaratkaisuja yrityksen IT-osastolle.

Tietomurtojen ja hakkeroinnin yleistyessä tulisi yritysten tehdä kaikkensa varautuakseen mahdollisiin tietomurtoihin sekä pitääkseen tärkeät tietonsa turvassa. Erityisesti sähköisen viestinnän tietosuojakysymykset ovat tässä opinnäytetyössä isossa roolissa.

Tutkimuksessa käytetyllä kyselyllä selvitetään muun muassa yritysten pääsynhallintaan, fyysiseen turvallisuuteen ja henkilöstöön liittyviä kysymyksiä. Kyselyllä kartoitetaan pk-yritysten tämän hetkistä tilannetta, minkä jälkeen kysymyksistä tehdään asianmukaiset päätelmät ja niihin liittyvät suositukset.

Tutkimus on toteutettu kyselytutkimuksena. Kyselyyn vastasi 20 pk-yritystä.

ASIASANAT:

tietoturva, tietosuoja, tietoturvallisuus, organisaatio, yritys

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Techonology | Business Data Communications and Information Security

2014 | 42 pages

Esko Vainikka

Saku Nuutinen ja Hans Lindström

INFORMATION SECURITY SURVEY FOR SMALL BUSINESSES

The purpose of this study is to help companies to identify security risks, improve security through general operational efficiency and rational management solutions to build a better IT department.

In the study we used a quantitative survey investigating corporate access control, physical security and personnel-related issues. We issued the survey to 20 SMEs about their current situation, and then analysed the results and made related recommendations.

According to the survey most of the even smallest SMEs acknowledge the risks involved in information security. Most of the SMEs also perform a satisfactory amount of information security measures considering the size of the company.

The significance of this survey is to help SMEs realise that information security is an important aspect of business and that it is important to consider and apply.

KEYWORDS:

information security, data security, organization, business

SISÄLTÖ

1 JOHDANTO **6**

2 YLEISESTI YRITYSTEN TIETOTURVASTA **8**
2.1 Tietoturvan osa-alueet 8
2.2 Tietoturvan tärkeys yrityksessä 9
2.3 Tietoturvariskien arviointi 9
2.4 Fyysinen turvallisuus 10
2.5 Välttämättömät perustoimenpiteet 11
2.6 Suositeltavat toimenpiteet 11

3 TIETOSUOJAN SOVELTAMINEN LIIKETOIMINNASSA **12**

4 KYSELYN TOTEUTTAMINEN **16**

5 TUTKIMUSTULOKSET **18**
5.1 Pääsynhallinta 19
5.2 Henkilöstö 21

6 JOHTOPÄÄTÖKSET **25**
6.1 Suositukset 25
6.2 Yhteenveto 26

LÄHTEET **27**

LIITTEET

Liite 1. Tietoturvakysely pk-yrityksille
Liite 2. Kyselyn vastaukset

KUVIOT

Kuvio 1. Yrityksen koko. 18
Kuvio 2. Yrityksen tietoturvaohjeistus. 19
Kuvio 3. Fyysinen pääsynhallinta. 19
Kuvio 4. Yrityksen fyysinen turvallisuus. 20

Kuvio 5.Rajattujen järjestelmien pääsynhallinta. 21
Kuvio 6. Yrityksen tietoturvasta vastaava henkilö. 21
Kuvio 7. Henkilöstön tietoturvakoulutus. 22
Kuvio 8. Henkilöstön taustojen tarkistus. 23
Kuvio 9. Salasanat. 23
Kuvio 10. Varmuuskopiot. 24

1 JOHDANTO

Yrityksen näkökulmasta tietoturvalla tarkoitetaan usein myyntiin, henkilöstöön ja yhteistyökumppaneihin liittyvien tietojen suojaamista. Tämä on liiketoiminnan kannalta elintärkeää. Huonosti hoidettu tietoturva saattaa aiheuttaa tietojen ajautumisen väärien henkilöiden käsiin, mikä tarkoittaa yleensä taloudellisia tappioita esimerkiksi maineen menetyksen kautta.

Jokaisen yrityksen asiakkaat varmasti tuntevat olevansa oikeutettuja omien henkilökohtaisten tietojensa salassa pysymiseen. Toisaalta myös työntekijän kannalta on tärkeää, että omat työhön liittyvät dokumentit ja sähköpostiviestit ovat turvassa. Näiden kahden kohderyhmän lisäksi myös jo olemassa olevilla ja potentiaalisilla liikekumppaneilla on omat olettamuksensa tietoturvan tasosta. Kaikki haluavat – tai ainakin tulisi haluta – varmistua siitä, ettei ota ylimääräisiä riskejä tehdessään yhteistyötä uuden tuttavuuden kanssa.

Kustannussyistä ei ehkä ole mahdollista luoda jokaiselle yritykselle aukotonta tietoturvajärjestelmää. Jokaiselle on kuitenkin mahdollista luoda järjestelmä, jolla saadaan haitallisten henkilöiden tai ohjelmien mielenkiinto siirrettyä helpompiin kohteisiin. Tässä opinnäytetyössä käsitellään asioita melko yleisvaltaisesti, mutta kuitenkin hieman enemmän pk-yritysten kuin isojen yritysten näkökulmasta.

Tutkimus on Webropol-sovelluksella tehty www-kysely. Pyrimme aluksi kartoittamaan yritysten tietoturvan tasoa. Kyselyssä käsitellään henkilöstöön ja organisaatioon liittyviä kysymyksiä. Myös fyysinen turvallisuus ja pääsynhallinta kuuluvat kyselyyn.

Tavoitteena on kehittää ratkaisuja tutkimustulosten perusteella havaittuihin tietoturvaongelmiin tai -puutteisiin.

Työmme liittyy suurempaan hankkeeseen, jossa pyritään selvittämään tietoturvallisuuden tilannetta Turun alueen pk-yrityksissä. Saimme työn toimeksiantona

Turun AMK:lta ja suuntasimme kyselyn Raision Yrittäjät ry:lle. Yhdistyksessä on yhteensä 373 jäsenyritystä.

Opinnäytetyötä tehdessä ei varsinaisesti ollut työnjakoa, vaan teimme kaiken yhdessä.

2 YLEISESTI YRITYSTEN TIETOTURVASTA

2.1 Tietoturvan osa-alueet

Tietoturva on hyvin laaja käsite ja se koostuu useasta eri osa-alueesta. Osa-alueita ovat

- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöstöturvallisuus
- tietoaineistoturvallisuus
- ohjelmistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus
- käyttöturvallisuus (Hakala 2006, 10).

Tietoturvallisuuden määritelmä perustuu pitkälti tiedon kolmen perusominaisuuden turvaamiseen. Nämä ovat luottamuksellisuus, eheys ja saatavuus. (Laaksonen ym. 2006, 17, Andress 2011, 4.)

Näillä yllämainituilla kolmella perusominaisuudella pyritään suojaamaan asianmukaisesti erilaiset tiedot ja palvelut niin, että hallitaan niihin liittyvät riskit ja taataan näin yrityksen menestyksekäs liiketoiminta.

Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan tiedon saannin rajoittamista vain niille henkilöille, joilla on siihen oikeus. Toinen osa luottamuksellisuutta on estää tiedon kulkeutuminen ns. ”vääriin käsiin”. Nämä kaksi seikkaa voidaan turvata erilaisilla autentikointimetodeilla, kuten henkilökohtaisilla tunnisteilla ja salasanoilla.

Eheys

Tiedon eheys tarkoittaa, että voidaan olla varmoja lähteestä tai lähettäjästä ja että tieto on totta. Liiketoiminnassa sekä luodaan että lähetetään valtavia määriä tietoa päivittäin. Tietojen tulisi siis pysyä ennallaan lähetettäessä tai siirrettäessä ja muutosten tekeminen niihin tulisi olla rajattu.

Saatavuus

Jotkin yritykset tai organisaatiot ovat täysin riippuvaisia tietojärjestelmien toiminnasta. Järjestelmä, joka ei ole käytettävissä silloin, kun sitä tarvitaan, on lähestulkoon tarpeeton. Ihminen on yleensä näissä saatavuuteen liittyvissä ongelmissa heikoin lenkki.

2.2 Tietoturvan tärkeys yrityksessä

Ymmärtääksemme täysin tietoturvan arvon, on ensiksi ymmärrettävä tiedon arvo ja sen lisäksi tietojen vaarantamisesta aiheutuvat seuraukset.

Yritys säilyttää arkaluonteista tietoa sekä työntekijöistään että asiakkaistaan, kuten palkkatietoja, taloudellisia tuloksia ja esimerkiksi liiketoimintasuunnitelmia tulevalle vuodelle. Ne voivat myös olla liikesalaisuuksia tai tutkimustuloksia, jotka antavat yritykselle kilpailuetua.

Yhä useammin tämä tieto varastoidaan ja käsitellään sähköisesti, jolloin luvattoman käytön riski kasvaa. Yrityksillä on siis omien tietojensa lisäksi vastuu myös asiakkaidensa tiedoista.

2.3 Tietoturvariskien arviointi

Säännöllisin väliajoin, tai kun merkittäviä muutoksia tapahtuu, tulee yrityksen suorittaa tietoturvariskien arviointia. Riskien arvioinnin tarkoituksena on määrit-

tää, mitä sellaista voisi tapahtua, mikä voisi aiheuttaa tappioita, ja saada tietoa siitä, miten, missä ja miksi tällainen tappio voisi syntyä. Arvioinnin olisi katettava kaikki riskit riippumatta siitä, onko niiden lähde yrityksen hallinnassa vai ei. (ISO/IEC 27005 2013.)

Itse arviointiprosessissa määritetään suojattavien kohteiden arvo ja niihin kohdistuvat uhat. Riskit voidaan arvioinnin perusteella asettaa tärkeysjärjestykseen ja yksilöidä niille käytettävissä olevat hallintakeinot. Tällaisen prosessin tarkoituksena on luoda mittari, jonka avulla voidaan seurata käytettyjä työtunteja ja kustannusten vaihtelua. Prosessimuotoisella mittaamisella saavutetaan yrityksen kannalta oleellista hyötyä sekä tietoturvallisuuden että toiminnan ohjauksen tasolla.

2.4 Fyysinen turvallisuus

Fyysinen turvallisuus perustuu kolmen pääkategorian suojelemiseen. Nämä pääkategoriat ovat tärkeysjärjestyksessä seuraavat: ihmiset, tieto ja laitteisto.

Ihmiset ovat listassa luonnollisesti ensimmäisenä, koska ihmiset ovat yrityksen tärkein voimavara. Työvoimaa ja varsinkin kokenutta työvoimaa on erittäin vaikeaa korvata nopeasti, jos ollenkaan. Helpoimmat toimenpiteet ihmisten suojelemiseksi ovat evakuointisuunnitelmat ja turvalliset toimintatavat.

Tiedon turvaaminen on toiseksi tärkeintä. Jos yrityksen hallussa olevat tiedot kuten sopimukset ja asiakastiedot katoavat eikä niistä ole varmuuskopioita, niitä on erittäin vaikeaa ja työlästä saada takaisin. Helpoiten tieto turvataan varmuuskopioinnilla ja varmistamalla, etteivät ulkopuoliset pääse käsiksi tietoon.

Viimeinen pääkategoria on laitteisto. Laitteisto on listalla kolmantena, koska jos laitteisto vikaantuu tai siihen kohdistuu muita ongelmia, on se helpompi, halvempi ja nopeampi korvata kuin ihmiset tai tieto. Laitteiston suojelemiseksi on syytä olla hälytys- ja valvontalaitteita, jotta esimerkiksi vesivahingon tai tulipalon sattuessa voidaan ryhtyä tarvittaviin toimenpiteisiin.

2.5 Välttämättömät perustoimenpiteet

Jokaiseen laitteeseen tulisi asentaa ajan tasalla olevat anti-virus- ja anti-spywareohjelmistot. Jotkin ohjelmistot ovat ilmaisia, toiset taas saattavat olla maksullisia. Ilmaisten joukosta voi myös löytyä riittävän tasokkaita, kunhan pitää huolen päivityksistä.

Päivittäminen viimeisimpään versioon on tärkeää. Se kannattaa hoitaa esimerkiksi yöllisillä ajastetuilla päivitysten tarkastuksilla. Päivitysten tarkastuksen jälkeen voidaan suorittaa vaikkapa järjestelmän virusskannaus.

Ohjelmistosta riippuen on mahdollista käyttää myös taustavalvontaa, joka on jatkuvasti päällä työaseman taustalla. Toiminto valvoo kaikkia koneeseen saapuvia ja koneesta lähteviä tiedostoja sekä tutkii tiedostot, jotka tallennetaan kiintolevylle. Taustavalvonta hyödyntää myös samaa tunnistetietokantaa kuin skannaus. Sen vuoksi virustorjuntaohjelmisto on erittäin tärkeää pitää ajan tasalla asentamalla kaikki päivitykset heti niiden julkaisun jälkeen.

2.6 Suositeltavat toimenpiteet

Jokaisen työntekijän tulisi ymmärtää tietoturvallisuuden merkitys ja ottaa pienet teot osaksi arkipäiväisiä rutiineja. Käyttäjien koulutuksella on suuri rooli siinä, miten nämä pienet teot lopulta otetaan käytäntöön.

Tilanteissa, joissa työntekijä ei esimerkiksi ole varma, mitä sähköpostin sisältämä liitetiedosto koskee, voisi vaikka soittaa lähettäjälle. Yleisestikin tulisi laatia toimintamallit erilaisille tilanteille. Käyttäjäkoulutuskin kantaa toki vain tiettyyn pisteeseen asti. Jotkin viruksia tai haittaohjelmia sisältävät sähköpostit voivat näyttää tulevan talon sisäisesti työtoverilta, vaikka ne eivät sitä olisikaan.

3 TIETOSUOJAN SOVELTAMINEN LIIKETOIMINNASSA

Henkilötietolaki

Henkilötietolain tarkoituksena on suojella yksityishenkilöiden yritykselle luovuttamia tietoja. Tällaisia tietoja ovat henkilökohtaiset ominaisuudet tai elinolosuhteita kuvaavat merkinnät. Lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. (Henkilötietolaki 523/1999.)

Lain soveltaminen

Henkilötietolakia sovelletaan, kun käsitellään henkilötietoja. Laki koskee viranomaisten, yritysten, järjestöjen, muiden yhteisöjen sekä yksityisten henkilöidenkin toimintaa.

Soveltamisen ulkopuolelle jää kuitenkin muutaman tyyppiset henkilötietojen käsittelyt. Ulkopuolelle jää tietyin rajoituksin henkilötietojen käsittely toimituksellisia ja taiteellisen ja kirjallisen ilmaisun tarkoituksia varten. Soveltamatta jätetään myös normaalia, vain henkilökohtaisessa tarkoituksessa tehtävää henkilötietojen käsittelyä. Tällaisella käsittelyllä tarkoitetaan vaikkapa ystäväpiirin osoitteiden tai puhelinnumeroiden ylläpitoa. (Tietosuojavaltuutettu 2001.)

Yrityksen vastuu

Henkilötietolain mukaan rekisterinpitäjä on yksi tai useampi henkilö, yhteisö, laitos tai säätiö, jonka käyttötarkoituksiin henkilörekisteri on perustettu ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi on lain mukaan säädetty rekisterinpito. Rekisterinpitäjä on vastuussa siitä, että henkilötietoja käsitellään lain vaatimusten mukaisesti.

Yritys on rekisterinpitäjä asiakkaidensa ja henkilöstönsä osalta. Yritys on siis vastuussa siitä, että tietojärjestelmät vastaavat lain vaatimuksia ja että henkilötietojen keräämiseen liittyvät vastuut ja tehtävät on jaettu asiallisesti. Yritystoiminnassa rekisterinpitäjänä ei voida pitää yksittäistä yrityksen palveluksessa olevaa työntekijää, joka kerää asiakkaiden henkilötietoja. (Tietosuojavaltuutettu 2001.)

Laki vaatii rekisterinpitäjää laatimaan henkilörekisteristä rekisteriselosteen, josta selviää

- rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot
- henkilötietojen käsittelyn tarkoitus
- kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä
- mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle
- kuvaus rekisterin suojauksen periaatteista.

Rekisteriseloste on pidettävä jokaisen saatavilla. Poikkeustilanteina on valtion turvallisuus ja puolustus, rikoksen ehkäiseminen tai selvitys taikka verotukseen tai julkiseen talouteen liittyvä valvontatehtävä (Henkilötietolaki 523/1999).

Henkilötietolain soveltaminen verkossa

Verkkopalveluiden käytöstä jäävät käyttäjien tiedot voivat myös kuulua henkilötietoihin. Kerättäessä henkilötietoja verkon kautta rekisteröidyllä käyttäjällä on oikeus tietää mihin tarkoitukseen ja miten hänen tietojaan käsitellään. Henkilörekisterin henkilötietojen laittaminen esimerkiksi kotisivuille vaatii asianomaisen henkilön suostumuksen tai jonkin lain antaman poikkeuksellisen oikeutuksen. (Tietosuojavaltuutettu 2001.)

Oikeus kerätä henkilötietoja

Henkilötietojen keräämiseen ja käsittelyyn vaaditaan henkilötietolaissa määritellyt edellytykset.

Henkilötietoja voidaan kerätä ja tallettaa:

- Kun henkilö on antanut siihen suostumuksensa.
- Kun rekisterinpitäjän ja henkilön välillä on asiallinen yhteys, kuten asiakassuhde tai asukassuhde. Henkilön on myös oman asiointinsa perusteella tiedettävä tämä.
- Kun oikeus henkilötietojen käsittelyyn perustuu muussa laissa säädettyyn tehtävään tai käsittelystä on säädetty laissa. (Tietosuojavaltuutettu 2001.)

Lisäksi henkilötietolain 4. luvussa (Henkilötietolaki 523/1999) on säädetty lisäedellytyksiä, joiden täyttyessä henkilötietoja voidaan käsitellä myös

- suoramarkkinoinnin ja muiden osoitteellisten lähetysten käsittelyä varten
- tieteellistä tutkimusta varten
- tilastointia varten
- sukututkimusta varten
- henkilömatrikkelin muodostamiseksi
- henkilöluottotietojen käsittelyä varten
- viranomaisten suunnittelu- ja selvitystehtäviä varten.

Henkilötietojen keräämistä ja käsittelyä ohjaavat myös useat muut lait, joten lainmukaisuuden varmistaminen vaatii myös muiden henkilötietojen käsittelyä koskevien lakien selvittämistä.

Valvonta

Henkilötietojen käsittelyyn liittyvää ohjausta, valvontaa, käsittelyä ja ratkaisuja yrityksissä suorittaa tietosuojavaltuutettu. Tietosuojavaltuutetulla on oikeus saa-

da kaikki henkilötiedot ja muut tiedot, jotka ovat tarpeellisia henkilötietojen käsittelyn lainmukaisuuden valvonnassa. Valtuutettu saa näin tarkistaa henkilötietorekistereitä ja myös käyttää siinä apuna asiantuntijoita. Myös tilanteessa, jossa rekisteröity haluaa käyttää tarkastusoikeuttaan tai tiedon korjaamista, tietosuojavaltuutettu voi antaa rekisterinpitäjälle tästä määräyksen (Henkilötietolaki 523/1999).

Tietosuojavaltuutetun virasto on asiantuntijaorganisaatio ja valvontaviranomainen. Virasto auttaa rekisteröityjä ja rekisterinpitäjiä tietosuojaan liittyvissä ongelmatilanteissa ja kysymyksissä.

Euroopan komissio antoi 4.11.2010 lausunnon uudesta lähestymistavasta koskien henkilötietoja. Uudistusehdotusta kehitetty useissa kokouksissa ja sen kehitys jatkuu edelleen. Tavoitteita ovat yksilön oikeuksien ja sisämarkkinaulottuvuuden lujittaminen, rikosasioissa tehtävää poliisi- ja oikeudellista yhteistyötä koskevien tietosuojasääntöjen tarkistaminen ja tietosuojan globaalin ulottuvuuden huomioon ottaminen. (Oikeusministeriö 2014.)

4 KYSELYN TOTEUTTAMINEN

Aloittaessamme kyselyn suunnittelun tavoitteena oli tuottaa mahdollisimman helposti luettava ja ymmärrettävä kysely. Kohderyhmä oli Raision seudun PK-yritykset, joiden henkilöstömäärä on 1-250 henkilöä. Tästä johtuen kysymysten oli oltava yksinkertaisia ja ymmärrettäviä pienillekin yrityksille, joissa ei välttämättä ole henkilöstöä, jolla on paljoakaan tietämystä tietoturvaan liittyvistä termeistä ja käsitteistä. Oli siis löydettävä tapa esittää kysymykset selkeästi ja myös selittää mahdolliset heille tuntemattomat termit sillä tavalla, että vastaajat varmasti ymmärtävät kysymykset. Tarkoituksena oli saada mahdollisimman vähän vastauksia valinnalla "En osaa sanoa". Tämä sen takia, että nämä vastaukset ovat kyselyn tuloksia tutkiessa vaikeampia analysoida kuin selkeät "Kyllä" ja "Ei".

Toinen tavoite kyselyä luodessa oli tehdä kyselystä sopivan pituinen. Kysely ei saanut olla liian pitkäkestoinen, jottei kyselyn vastaajan mielenkiinto laske ennen kuin hän on vastannut kaikkiin kysymyksiin. Toisaalta kysely ei myöskään voinut olla liian lyhyt, jotta saadaan kerättyä tarpeeksi tietoa, jota tutkia. Tavoitepituudeksi kyselyn kestolle otimme 15 minuuttia. Kyselyyn tuli lopulta 43 eri kohtaa, joiden vastausvaihtoehdot olivat joko "Kyllä", "Ei" tai "En osaa sanoa". Kaksi kysymystä sisälsi monivalintakysymyksen. Kyselylomake on liitteenä 1.

Kysymyksiä suunnitellessa käytimme apuna tietoturva-auditointilomaketta Standardized Information Gathering Questionnaire (Shared Assessments 2010), jonka avulla osasimme suunnitella kyselyn rungon ja osa-alueet, joihin kysymykset liittyivät. Käytössämme oli lomakkeen viimeinen ilmainen versio 6.0. Lomakkeessa oli useita satoja yksityiskohtaisia kysymyksiä, joista valitsimme tärkeimmät ja mielestämme helpoiten ymmärrettävät. Kysymykset perustuvat ISO 27001-standardiin (ISO/IEC 27001 2013). Tämän jälkeen oli mutkatonta suunnitella ja luoda toimiva kysely.

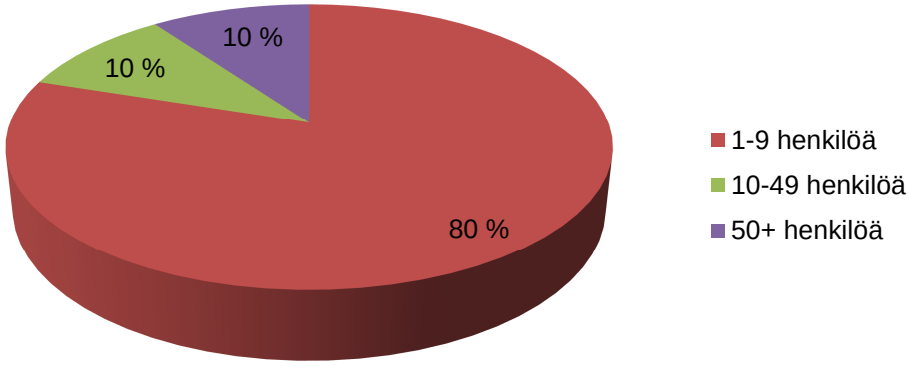
Kysely toteutettiin käyttämällä Webropol-kysely- ja analysointisovellusta, jotta varsinaisen kyselyn luomisesta tehtäisiin nopeaa ja yksinkertaista. Toteutus ja

julkaisu onnistuikin varsin vaivattomasti ja ilman ongelmia. Webropolin analysointityökalut myös helpottavat saatujen vastausten tutkimista ja johtopäätösten tekemistä.

5 TUTKIMUSTULOKSET

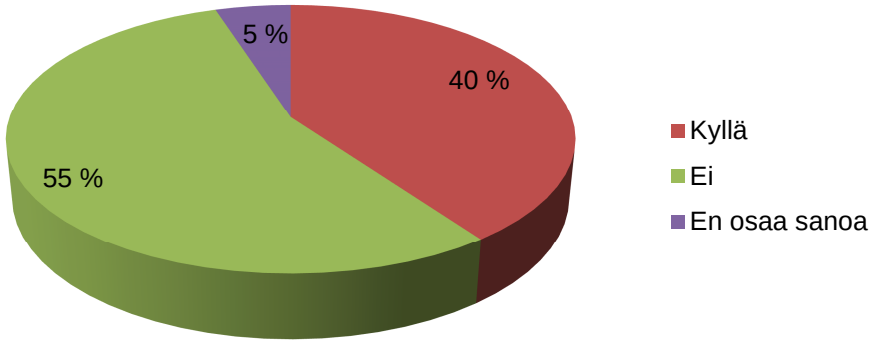
Kysely lähetettiin Raision Yrittäjät ry:n jäsenyrityksille, joita on 373. Kysely avattiin yhteensä 48 kertaa, mutta sen avanneista 28 jätti täyttämisen kesken. Vastausprosentti jäi siis odotettua alhaisemmaksi. Kaikkiin kysymyksiin vastaaminen oli pakollista, mikä saattoi myös vaikuttaa keskeytettyjen kyselyiden määrään.

Vastanneista yrityksistä 80 % oli 1-9 henkilön ns. mikroyrityksiä, 10 % pieniä ja 10 % keskisuuria yrityksiä (kuvio1).



Kuvio 1. Yrityksen koko.

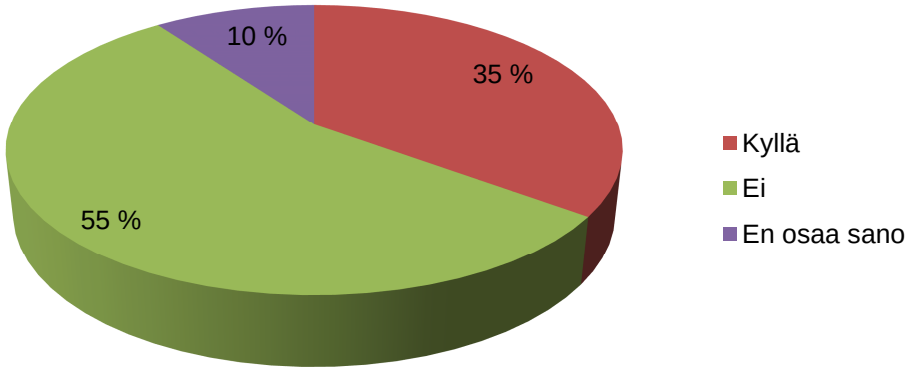
Kysyttäessä, onko yrityksillä tietoturvaohjeistusta, saimme seuraavat tulokset (kuvio 2). Yli puolilla vastanneista yrityksistä (55 %) ei ole tietoturvaohjeistusta, hieman alle puolella (40 %) taas sellainen on ja loput yrityksistä (5 %) eivät osanneet sanoa.



Kuvio 2. Yrityksen tietoturvaohjeistus.

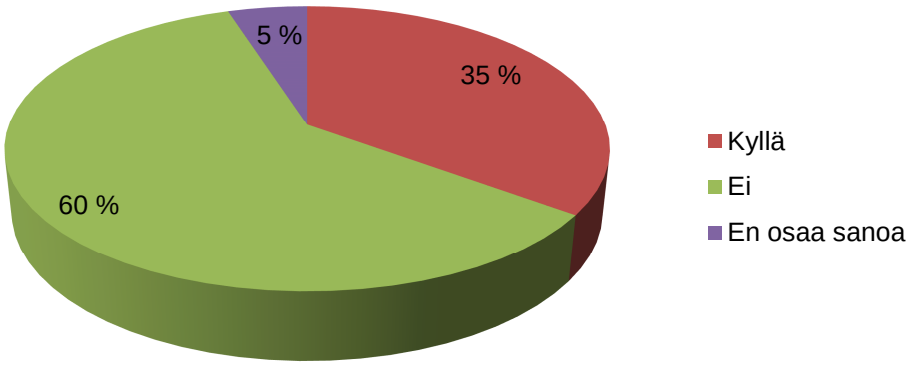
5.1 Pääsynhallinta

Kysyttäessä onko yrityksillä elektroninen järjestelmä fyysistä pääsynhallintaa varten, saimme seuraavat tulokset (kuvio 3). Yli puolilla yrityksistä (55 %) ei ole minkäänlaista elektronista järjestelmää, noin kolmasosalla yrityksistä (35 %) on vastaava järjestelmä ja pieni osa yrityksistä (10 %) ei osannut vastata kysymykseen.



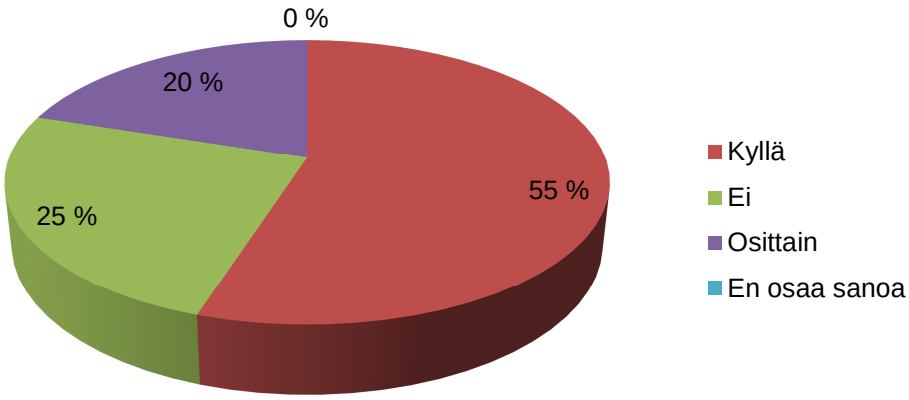
Kuvio 3. Fyysinen pääsynhallinta.

Kysyttäessä onko yrityksillä fyysisen turvallisuuden suunnitelmaa, saimme seuraavat tulokset (kuvio 4). Kolmasosalla yrityksistä (35 %) on fyysisen turvallisuuden suunnitelma, reilusti yli puolilla yrityksistä (60 %) ei ole suunnitelmaa ja pieni määrä yrityksistä (5 %) ei osannut sanoa, onko heillä fyysisen turvallisuuden suunnitelmaa.



Kuvio 4. Yrityksen fyysinen turvallisuus.

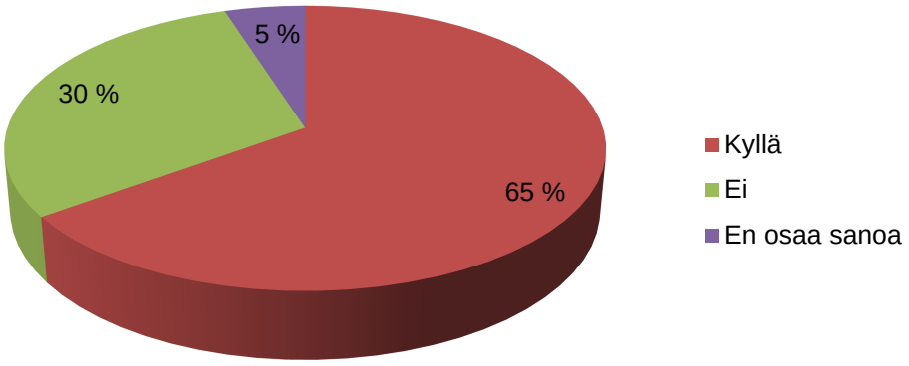
Kysyttäessä yrityksiltä vaaditaanko yrityksissä rajattuihin järjestelmiin ja tietoihin salasanaa, saimme seuraavat tulokset (kuvio 5). Yli puolet yrityksistä (55 %) vaativat salasanan rajattuihin järjestelmiin, viidesosa yrityksistä (20 %) vaatii osittain salasanaa ja neljäsosa yrityksistä (25 %) ei vaadi salasanaa.



Kuvio 5.Rajattujen järjestelmien pääsynhallinta.

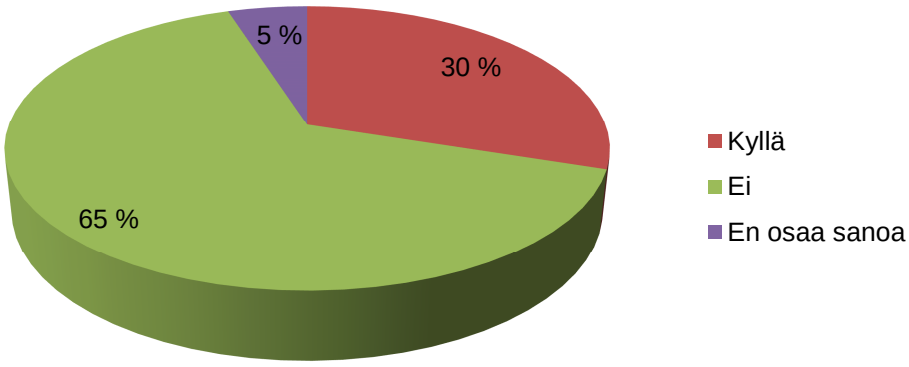
5.2 Henkilöstö

Kysyttäessä onko yrityksillä tietoturvasta vastaavaa henkilöä, saimme seuraavat tulokset (kuvio 6). Noin kahdella kolmesta yrityksestä (65 %) on tietoturvasta vastaava henkilö, kolmasosalla yrityksistä (30 %) ei ole vastaavaa ja pieni osa yrityksistä (5 %) ei osannut sanoa, onko heillä kyseistä henkilöä.



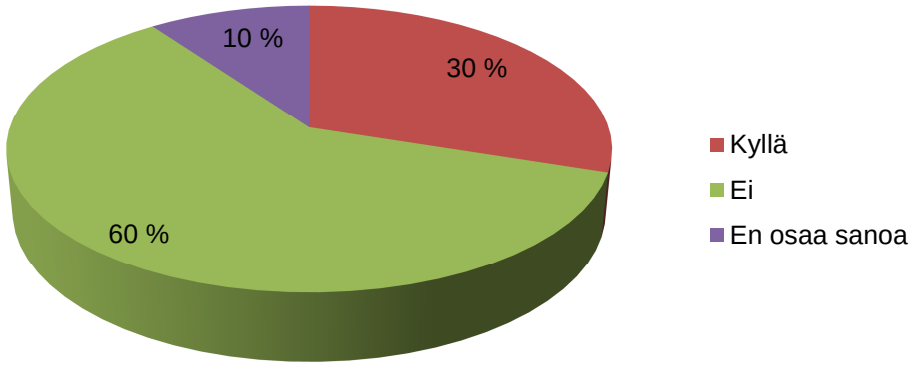
Kuvio 6. Yrityksen tietoturvasta vastaava henkilö.

Henkilöstön tietoturvakoulutusta käsittelevässä kysymyksessä halusimme tietää, järjestetäänkö sellaista ollenkaan (kuvio 7). Vastausten perusteella yli puolissa yrityksissä (65 %) ei järjestetä, joka kolmannessa järjestetään ja loput eivät osanneet sanoa.



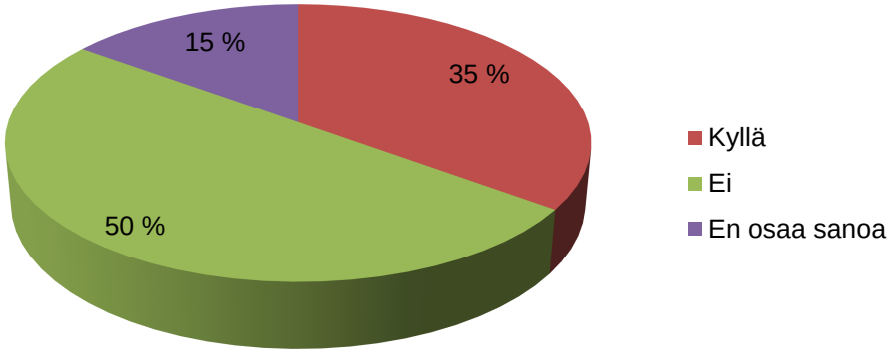
Kuvio 7. Henkilöstön tietoturvakoulutus.

Kysyttäessä tarkistetaanko henkilöstön taustat ennen pääsyä tietojärjestelmiin ja -palvelimiin (kuvio 8) yli puolet vastasi ”Ei” (60 %). Kolmasosa ”Kyllä” ja loput 10 % ei osannut sanoa.



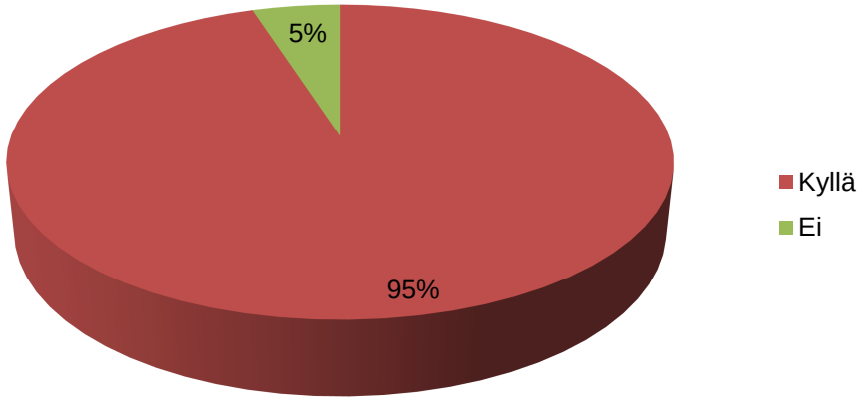
Kuvio 8. Henkilöstön taustojen tarkistus.

Kysyimme myös, vaaditaanko yrityksessä monimutkaisia salasanoja, joka tarkoittaa pieniä ja isoja kirjaimia sekä erikoismerkkejä sisältävää salasanaa. 35 % vastaajista ilmoitti ne pakollisiksi ja 15 % ei osannut sanoa. Puolissa yrityksistä ne eivät olleet vaadittuja (kuvio 9).



Kuvio 9. Salasanat.

Lähettämässämme kyselyssä oli kaikkiaan yli neljäkymmentä kysymystä. Analysoitavaksi otimme kuitenkin vain kymmenen, joista viimeisessä (kuvio 10) käsittelimme varmuuskopiointia. Kysymys sisälsi sekä tiedostojen että järjestelmien varmuuskopioinnin ja lähes kaikki (95 %) vastaajista kertoivat yrityksen varmuuskopioinnin olevan kunnossa. Vain yhdessä kahdestakymmenestä se ei ollut (5 %).



Kuvio 10. Varmuuskopiot.

Vastaukset kaikkiin kysymyksiimme on esitetty liitteessä 2. Vastauksia ei ole jaoteltu yritysten koon mukaan johtuen pienestä vastausten määrästä.

6 JOHTOPÄÄTÖKSET

Analysoitavien vastausten määrä jäi haluttua pienemmäksi, kun vain parikymmentä kyselyn vastaanottanutta täytti sen kokonaan. Tuloksista voidaan kuitenkin muodostaa jonkinlainen kokonaiskuva tietoturva-asioiden tasosta tällä hetkellä yrityksissä. Täytyy kuitenkin ottaa huomioon, että 80 % yrityksistä oli alle 10 hengen mikroyrityksiä, joten vastaukset ovat myös sen mukaisia.

Odotettavissa oli, ettei pienten yritysten henkilökunnasta löydy riittävää käytännön osaamista käyttämässämme kyselyssä käsiteltäviin aiheisiin. Riskit todennäköisesti tiedostetaan, mutta resurssien rajallisuuden vuoksi niihin ei voida panostaa riittävästi aikaa tai rahaa. Kolmansien osapuolien apuunkin turvaudutaan yleensä vasta, kun ongelma on jo olemassa.

Voidaan todeta, että puolet tai jopa kaksi kolmesta yrityksestä ovat tietoisia tietoturvaan liittyvistä riskeistä. Positiivisesti yllättävää oli huomata, että mm. 65 %:lla vastanneista yrityksistä oli erikseen tehtävään nimetty tietoturvavastaava ja että vain yhdessä yrityksessä ei tehdä säännöllistä varmuuskopiointia.

Pääsynhallintaan liittyvissä kysymyksissä enemmistö ilmoitti, ettei heillä ole minkäänlaista elektronista järjestelmää tai fyysisen turvallisuuden suunnitelmaa (esim. turvakamerat tai kulunvalvontajärjestelmät). Yritysten kokoon nähden tällainen on kuitenkin ymmärrettävää, sillä suurimmalle osalle vastaajista kyseiset järjestelmät saattavat olla kalliita tai tarpeettomia.

6.1 Suositukset

Näiden kyselytulosten perusteella suosittelemme yritysten yleisen tietoturvakoulutuksen ja -tiedottamisen lisäämistä. Esimerkiksi kerran vuodessa olisi hyvä pitää jonkinlaista koulutusta, jolla pidettäisiin työntekijät ajan tasalla tietoteknisen maailman muuttuvista tietoturvariskeistä. Kustannuksiin nähden tällainen koulutus on yrityksille hyödyllistä.

Tietoturva-asioista vastaavan henkilön nimeämistä suosittelemme lähinnä isommille yrityksille (enemmän kuin 10 työntekijää). Alle kymmenen henkilön yrityksissä siitä ei välttämättä ole kuluihin nähden tarpeeksi hyötyä.

Suosittelemme yrityksiä vaatimaan työntekijöiltään monimutkaisia salasanoja. Salasanat olisi myös syytä vaihtaa vähintään 90 päivän välein. Tätä käytäntöä on helppo tietotekniikan avulla toteuttaa sekä valvoa. Monimutkaiset salasanat ovat myös tärkeä asia yrityksen tietoturvan kehittämisessä ja turvallisuuden luomisessa.

6.2 Yhteenveto

Tietoturva-aiheista teoriaa on tarjolla nykyään niin paljon, että on jokseenkin haastavaa lähteä rajaamaan tällaiseen työhön soveltuvaa materiaalia. Pyrimme kuitenkin työssämme käsittelemään vain oleellisimmat käytännön perusteet pienten yritysten näkökulmasta. Kyselyn rajaamisella oli helppo aloittaa, sillä saimme siitä pohjan työssä käsiteltäville aiheille.

Tulevaisuudessa kysely pitäisi uusia ja pyrkiä kaikin keinoin saamaan kaikki jäsenyritykset vastaamaan siihen. Vasta sen jälkeen voidaan tehdä johtopäätöksiä tietoturvallisuuden tilasta.

LÄHTEET

Andress, J. 2011. The Basics of Information Security – Understanding the Fundamentals of Infosec in Theory and Practice. Waltham: Elsevier Inc.

Hakala, M.; Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docento.

Henkilötietolaki 22.4.1999/523.

ISO/IEC 27005 2013. Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta.

ISO/IEC 27001 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallinta-järjestelmät. Vaatimukset.

Kissel, R. 2009. Small Business Information Security: The Fundamentals. Viitattu 21.3.2014. http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf.

Laaksonen, M.; & Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita Publishing Oy.

Mindfulsecurity.com – Why is information security important. Viitattu 20.3.2014. http://mindfulsecurity.com/2009/07/01/why-is-information-security-important/.

Oikeusministeriö 2014. Euroopan unionin tietosuojalainsäädännön uudistaminen. Viitattu 13.5.2014. http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/euroopanunionintietosuojalainsaadannonuudistaminen.html.

Piirainen, H. 2013. Tietoturvatietoisuuden kartoitus yrityksen erikoisosastoilla. Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Leppävaara: Laurea-ammattikorkeakoulu. Viitattu 21.3.2014.
http://urn.fi/URN:NBN:fi:amk-201305209671.

Shared Assessments 2010. Standardized Information Gathering Questionnaire. Viitattu 23.5 2014. http://listserv.educause.edu/cgi-bin/wa.exe?INDEX.

Seppänen, O. 2012. Tietoturvallisuuden kehittäminen yrityksessä. Viitattu 18.3.2014. https://publications.theseus.fi/bitstream/handle/10024/45967/Seppanen_Olli.pdf?sequence=1.

Tietosuojavaltuutettu 2001. Ota oppaaksi henkilötietolaki! Viitattu 9.4.2014. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq8WnQ7/Ota_oppaaksi_henkilotietolaki.pdf.

University of Miami. 2008. Confidentiality, Integrity and Availability (CIA). Viitattu 18.3.2014 http://it.med.miami.edu/x904.xml.

LIITTEET

Liite 1. Tietoturvakysely pk-yrityksille

Organisaatio

1. Tietoturvaohjeistuksella tarkoitetaan käytäntöjä koskien sähköpostia, varmuuskopioita, virustorjuntaa jne.

Onko yityksellänne tietoturvaohjeistus? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

2. Onko yrityksenne tietoturvaohjeistus löydettävissä helposti? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

3. Onko ulkopuolisilla henkilöillä pääsy tietojärjestelmiin tai tiedostoihin? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

4. Onko yrityksessänne tietoturvasta vastaavaa henkilöä? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

5. Edellyttääkö yrityksenne luottamuksellisuus- tai salassapitosopimusta kolmansilta osapuolilta? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

6. Onko olemassa sopimuksia ulkopuolisten palveluntarjoajien kanssa, joilla on pääsy tietojärjestelmiin ja tiedostoihin? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

Henkilöstö

7. Järjestetäänkö henkilöstölle tietoturvakoulutusta? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

8. Täytyykö uusien työntekijöiden allekirjoittaa: *

- ☐ salassapitosopimus
- ☐ luottamuksellisuussopimus
- ☐ käyttöehtosopimus
- ☐ ei tarvitse allekirjoittaa
- ☐ en osaa sanoa

9. Tarkistetaanko henkilöstön taustat ennen pääsyä tietojärjestelmiin ja -palvelimiin? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

10. Jos tarkistetaan, sisältyykö siihen rikosrekisteri? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

11. Jos tarkistetaan, sisältyykö siihen huumetesti? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

12. Onko olemassa kurinpitomenettelyä, jos tietoturvaohjeistusta laiminlyödään? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

Fyysinen turvallisuus

13. Fyysisellä turvallisuudella tarkoitetaan esimerkiksi kulunvalvontaa ja hälytyslaitteita.

Onko olemassa fyysisen turvallisuuden suunnitelmaa? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

14. Onko olemassa: *

- ☐ sisään- ja ulostulo-ovien hälytysjärjestelmää?
- ☐ hätäuloskäynnit, joista voidaan vain poistua?
- ☐ valvontakamera, jonka tiedot säilyvät ainakin 90 päivän ajan?
- ☐ palonsammutusjärjestelmä?
- ☐ savunilmaisin?
- ☐ en osaa sanoa

15. Onko olemassa elektroninen järjestelmä (avainkortti, avaimenperä, biometrinen lukija, numerokoodilukot, jne.), jolla valvotaan pääsyä tiloihin? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

Pääsynhallinta

16. Pitääkö salasanan pituus olla vähintään kahdeksan merkkiä? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

17. Monimutkainen salasana tarkoittaa salasanaa, joka sisältää isoja sekä pieniä kirjaimia, numeroita ja erikoismerkkejä.

Vaaditaanko monimutkaisia salasanoja? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

18. Meneekö salasana vanhaksi vähintään 90 päivän jälkeen? *

- ◯ Kyllä
- ◯ Ei

◯ En osaa sanoa

19. Onko salasana vaihdettava ensimmäisen kirjautumisen yhteydessä? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

20. Meneekö käyttäjätili lukkoon jos salasana/käyttäjätunnus on syötetty väärin 3-5 kertaa? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

21. Voiko käyttäjätunnus sisältää henkilökohtaista tietoa (henkilötunnus, nimi yms)? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

Pääsynhallinta

22. Poistetaanko tai lukitaanko käyttämättömät käyttäjätunnukset 90 päivän sisällä? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

23. Onko pääsy järjestelmiin rajoitettu fyysisen sijainnin mukaan? *

◯ Kyllä

◯ Ei

◯ Osittain

◯ En osaa sanoa

24. Suljetaanko istunto jos se on ollut käyttämätön 15 minuuttia? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

25. Rajatuilla järjestelmillä tarkoitetaan yrityksen arkaluontoista tietoa sisältäviä järjestelmiä.

Vaaditaanko rajattuihin järjestelmiin ja tietoihin salasana? *

- ◯ Kyllä
- ◯ Ei
- ◯ Osittain
- ◯ En osaa sanoa

26. Etäkäytöllä tarkoitetaan tietokoneen käyttöä etänä verkon yli.

Onko etäkäyttö sallittu? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

27. Sallitaanko vain yrityksen omistamien laitteiden etäyhteydet? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

Pääsynhallinta

28. Sallitaanko tietojen kopiointi etälaitteeseen? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

29. Kerätäänkö asiakkaista henkilökohtaisia tietoja? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

30. Ilmoitetaanko yksittäisille henkilöille jos/kun heidän tietojaan kerätään? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

Viestinnän ja toimintojen hallinta

31. Onko kolmannen osapuolen tekijöillä pääsy tietojärjestelmiin ja tiedostoihin (suorittaako kolmas osapuoli varmuuskopiointia, laitteistohuoltoa ym.)? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

32. Vaaditaanko kolmannen osapuolen tekijöiltä luottamuksellisuus ja/tai salassapitosopimus? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

33. Varmuuskopioinnilla tarkoitetaan tapahtumaa, jossa jokin tärkeä tieto kopioidaan ja varastoidaan. Jos alkuperäinen tieto häviää tai tuhoutuu, voidaan tieto palauttaa varmuuskopioista.

Otetaanko tiedostoista ja järjestelmistä varmuuskopiot? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

34. Säilytetäänkö varmuuskopioita muualla kun yrityksen omissa tiloissa? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

35. Testataanko varmuuskopioiden toimivuus säännöllisesti, vähintään kerran vuodessa? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

36. Suoritetaanko yrityksen omistamista medioista (USB-tikut jne.) inventaario? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

Viestinnän ja toimintojen hallinta

37. Tuhotaanko käytöstä poistettavien laitteiden tietosisältö? *

◯ Kyllä

◯ Ei

◯ En osaa sanoa

38. Onko käytössä virustorjuntaohjelmistoa? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

39. Onko käytössä normaalit käyttöjärjestelmän tarkistukset tietoturvariskien varalta? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

40. Korjauspäivityksillä tarkoitetaan käyttöjärjestelmälle tarkoitettuja päivityksiä, joiden tarkoituksena on parantaa käyttöjärjestelmän turvallisuutta ja toimintaa.

Onko käytössä ajanmukaiset korjauspäivitykset(patchit)? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

41. Onko käytössä ulkoisia verkkoyhteyksiä (Internet, extranet, etc.)? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

42. Onko käytössä langatonta verkkoteknologiaa? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

43. WPA2 on langattomien verkkojen tietoturvaratkaisu, joka tarjoaa vahvan salauksen.

Onko langaton yhteys salattu vahvalla tavalla (WPA2 tai tehokkaampi)? *

- ◯ Kyllä
- ◯ Ei
- ◯ Ei ole langatonta yhteyttä

Yrityksen tiedot

44. Yrityksen koko *

- ◯ 1-9 henkilöä

◯ 10-49 henkilöä

◯ 50+ henkilöä

45. Jos haluatte tietää miten yrityksenne pärjäsi kyselyssä, voitte jättää yhteystiedot alapuolelle:

Yrityksen nimi

_____

Sähköpostiosoite

_____

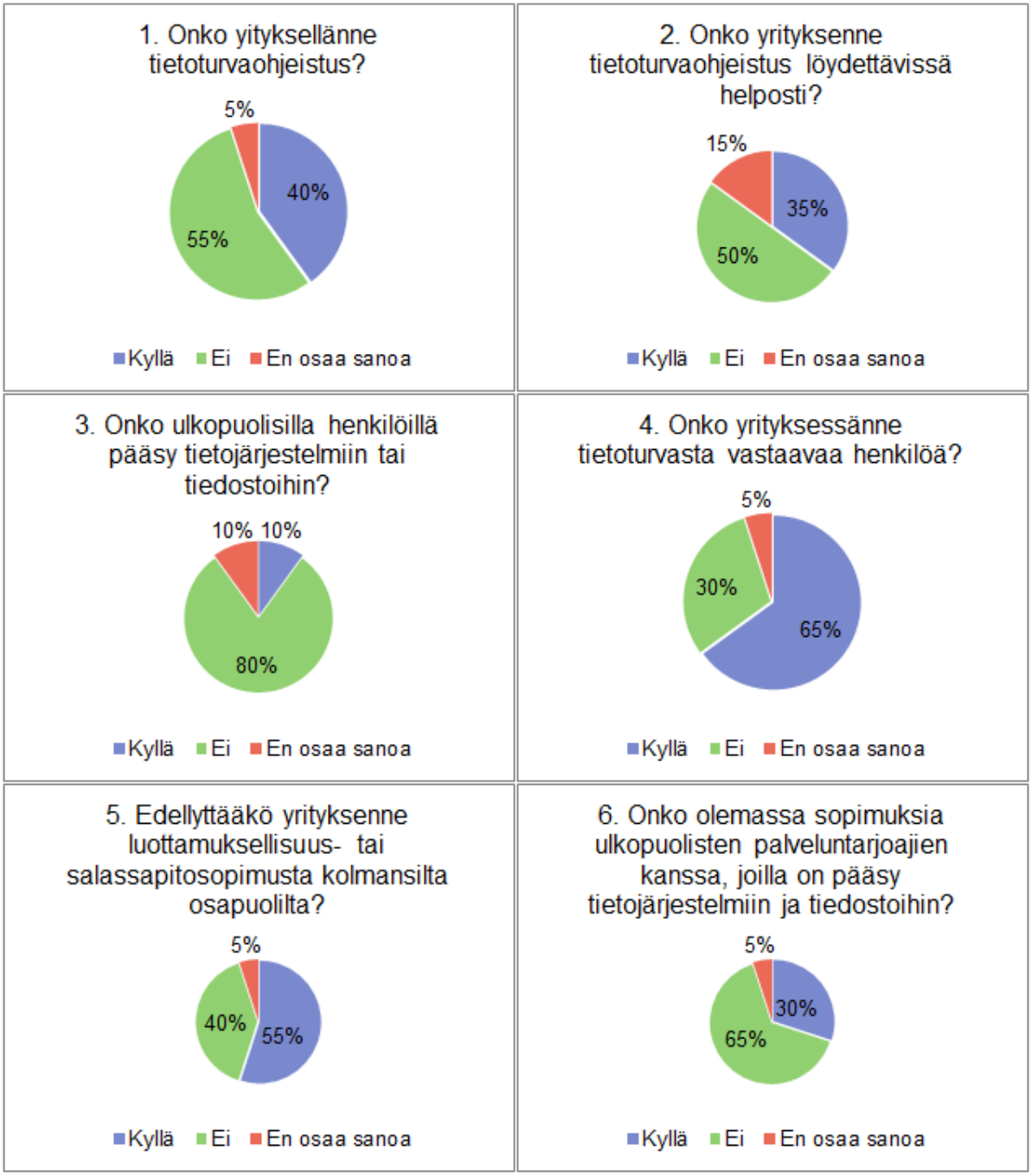
46. Palaute:

_____

_____

_____

Liite 2. Kyselyn vastaukset



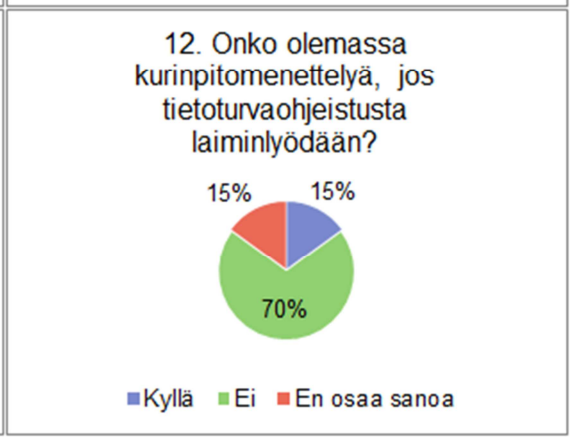

7. Järjestetäänkö henkilöstölle tietoturvakoulutusta?
5%
30%
65%
Kyllä
Ei
En osaa sanoa


8. Täytyykö uusien työntekijöiden allekirjoittaa:
15%
30%
50%
20%
0%
salassapitosopimus
luottamuksellisuussopimus
käyttöehtosopimus
ei tarvitse allekirjoittaa
en osaa sanoa

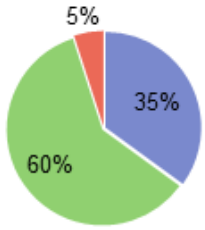

9. Tarkistetaanko henkilöstön taustat ennen pääsyä tietojärjestelmiin ja -palvelimiin?
10%
30%
60%
Kyllä
Ei
En osaa sanoa


10. Jos tarkistetaan, sisältyykö siihen rikosrekisteri?
10%
15%
75%
Kyllä
Ei
En osaa sanoa


11. Jos tarkistetaan, sisältyykö siihen huumetesti?
15%
85%
Kyllä
Ei
En osaa sanoa


12. Onko olemassa kurinpitomenettelyä, jos tietoturvaohjeistusta laiminlyödään?
15%
15%
70%
Kyllä
Ei
En osaa sanoa

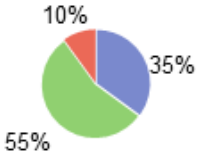
13. Onko olemassa fyysisen turvallisuuden suunnitelmaa?



Kyllä Ei En osaa sanoa

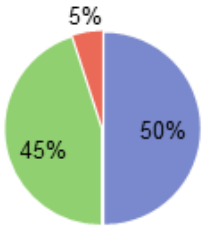
14. Onko olemassa:

15. Onko olemassa elektroninen järjestelmä (avainkortti, avaimenperä, biometrinen lukija, numerokoodilukot, jne.), jolla valvotaan pääsyä tiloihin?



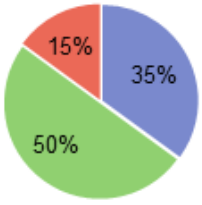
Kyllä Ei En osaa sanoa

16. Pitääkö salasanan pituus olla vähintään kahdeksan merkkiä?



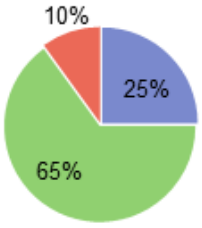
Kyllä Ei En osaa sanoa

17. Vaaditaanko monimutkaisia salasanoja?



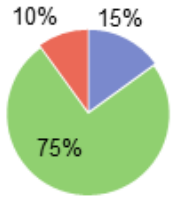
Kyllä Ei En osaa sanoa

18. Meneekö salasana vanhaksi vähintään 90 päivän jälkeen?

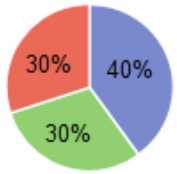


Kyllä Ei En osaa sanoa

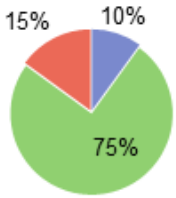
19. Onko salasana vaihdettava ensimmäisen kirjautumisen yhteydessä?



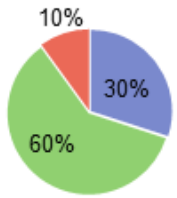
20. Meneekö käyttäjätili lukkoon jos salasana/käyttäjätunnus on syötetty väärin 3-5 kertaa?



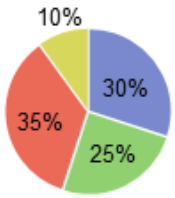
21. Voiko käyttäjätunnus sisältää henkilökohtaista tietoa (henkilötunnus, nimi yms)?



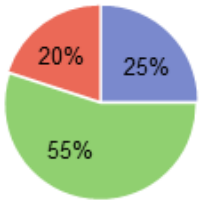
22. Poistetaanko tai lukitaanko käyttämättömät käyttäjätunnukset 90 päivän sisällä?



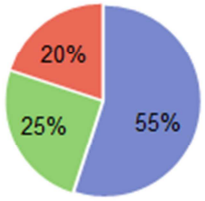
23. Onko pääsy järjestelmiin rajoitettu fyysisen sijainnin mukaan?



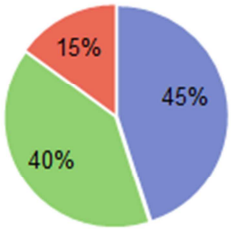
24. Suljetaanko istunto jos se on ollut käyttämätön 15 minuuttia?



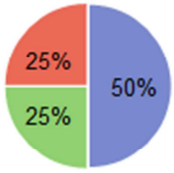
25. Vaaditaanko rajattuihin järjestelmiin ja tietoihin salasana?



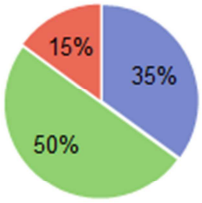
26. Onko etäkäyttö sallittu?



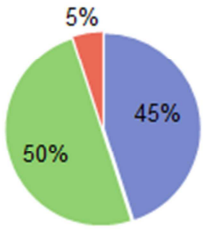
27. Sallitaanko vain yrityksen omistamien laitteiden etäyhteydet?



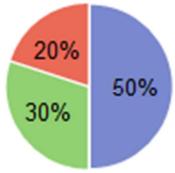
28. Sallitaanko tietojen kopiointi etälaitteeseen?



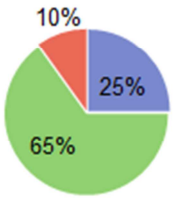
29. Kerätäänkö asiakkaista henkilökohtaisia tietoja?



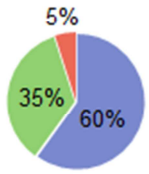
30. Ilmoitetaanko yksittäisille henkilöille jos/kun heidän tietojaan kerätään?



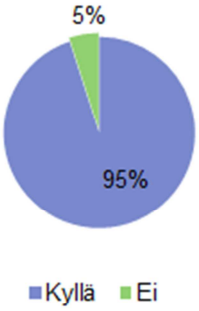
31. Onko kolmannen osapuolen tekijöillä pääsy tietojärjestelmiin ja tiedostoihin?



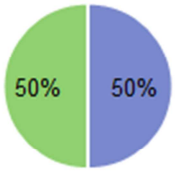
32. Vaaditaanko kolmannen osapuolen tekijöiltä luottamuksellisuus ja/tai salassapitosopimus?



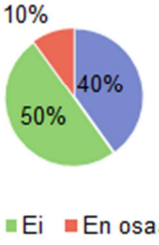
33. Otetaanko tiedostoista ja järjestelmistä varmuuskopiot?



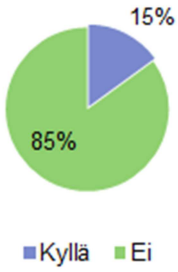
34. Säilytetäänkö varmuuskopioita muualla kun yrityksen omissa tiloissa?



35. Testataanko varmuuskopioiden toimivuus säännöllisesti, vähintään kerran vuodessa?



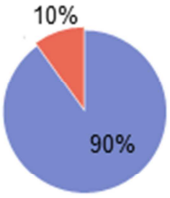
36. Suoritetaanko yrityksen omistamista medioista (USB-tikut jne.) inventaario?



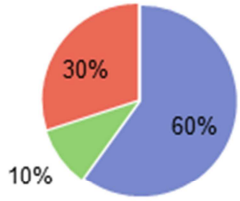
37. Tuhotaanko käytöstä poistettavien laitteiden tietosisältö?

38. Onko käytössä virustorjuntaohjelmistoa?

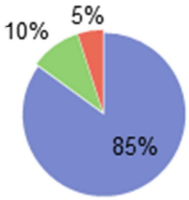
39. Onko käytössä normaalit käyttöjärjestelmän tarkistukset tietoturvariskien varalta?



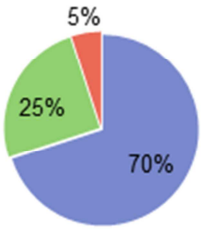
40. Onko käytössä ajanmukaiset korjauspäivitykset(patchit)?



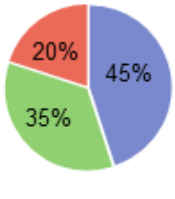
41. Onko käytössä ulkoisia verkkoyhteyksiä (Internet, extranet, etc.)?



42. Onko käytössä langatonta verkkoteknologiaa?



43. Onko langaton yhteys salattu vahvalla tavalla (WPA2 tai tehokkaampi)?



44. Yrityksen koko